Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Implementation of the	)	CC Docket No. 96-115
Telecommunications Act of 1996:	)	
	)	
Telecommunications Carriers' Use	)	
of Customer Proprietary Network	)	
Information and Other Customer Information	)	
	)	
IP-Enabled Services	)	WC Docket No. 04-36

COMMENTS OF QWEST COMMUNICATIONS INTERNATIONAL INC.
TO FURTHER NOTICE OF PROPOSED RULEMAKING

Craig J. Brown
Kathryn Marie Krause
Suite 950
607 14th Street, N.W.
Washington, DC 20005
303-383-6651

Attorneys for

QWEST COMMUNICATIONS
INTERNATIONAL INC.

July 9, 2007

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Implementation of the	)	CC Docket No. 96-115
Telecommunications Act of 1996:	)	
	)	
Telecommunications Carriers' Use	)	
of Customer Proprietary Network	)	
Information and Other Customer Information	)	
	)	
IP-Enabled Services	)	WC Docket No. 04-36

COMMENTS OF QWEST COMMUNICATIONS INTERNATIONAL INC.
TO FURTHER NOTICE OF PROPOSED RULEMAKING

I. INTRODUCTION AND SUMMARY

The Federal Communications Commission ("Commission" or "FCC") need not expand its Customer Proprietary Network Information ("CPNI") rules beyond those amendments reflected in the Commission's *April 2007 CPNI Order*.[1] Indeed, most of the proposals contained in the *2007 CPNI Further Notice* have already been publicly noticed for comment; and carriers, including Qwest, have overwhelmingly opposed them.[2]

---

[1] *See In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115 and WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22, rel. Apr. 2, 2007 ("*April 2007 CPNI Order*" or "*2007 CPNI Further Notice*" as appropriate).

[2] The Commission has already sought and received comment on issues pertaining to government-mandated passwords (including the adoption of a broad prescription), required audit trails, the de-identification of information issue, and mandated retention/destruction of customer information. *See, e.g.*, Comments of Qwest Communications International Inc. to Additional Customer Proprietary Network Information Rulemaking, filed Apr. 28, 2006 ("Qwest 2006 Comments") in *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115. The "new" subject introduced by the instant *2007 CPNI Further Notice* has to do with removing personal information from mobile devices.

When married with long-standing carrier attention to the privacy interests of their customers, the Commission's recent rule amendments provide more-than-sufficient protections for the responsible management of customer information. There is, after all, no record that carriers act in a chronically casual manner in the treatment of customer information or negligently with regard to its release. Additional CPNI regulation would only operate to unduly interfere with the carrier-customer relationship -- a relationship that both parties hope will be responsive, efficient and satisfying. Building unnecessary protective fortresses around the exchange of information between carriers and their customers, with a suppression of mutually-desirable speech, is not in the public interest. Nor is it necessary from a historical, legal or policy perspective.

Over two decades ago, prior even to the divesture of AT&T,[3] and continuing to this day, Qwest has taken reasonable, prudent steps to protect its customer information and to safeguard it from unauthorized disclosure. Qwest has instituted methods and procedures, as well as security tools and controls, to support and confirm its dedication to protecting information about its customers and their associated privacy interests.

A carrier's ability to communicate with its customers responsively and in an educated manner depends on the carrier's access to its customer information. Accurate billing and revenue generation also require a carrier to efficiently access such information. Clearly,

---

[3] While Congressional oversight of CPNI did not occur until 1996, Qwest -- a successor to U S WEST, a Bell Operating Company ("BOC") -- has long had its use of CPNI regulated by the Commission. *See In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115 and 96-149, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8068-70 ¶ 7 and associated footnote references (1998) ("*1998 CPNI Order*"), *on recon.*, 14 FCC Rcd 14409 (1999) ("*CPNI Reconsideration Order*"), *vacated sub nom. U S WEST v. FCC*, 182 F.3d 1224 (10th Cir. 1999), *cert. denied*, 530 U.S. 1213 (2000) ("*U S WEST v. FCC*").

customer information is a significant common carrier asset. Protecting that asset is critical with respect to customer trust and shareholder fiduciary expectations. And protect that asset Qwest does. Qwest employs safeguards that range from technical system controls, to policy and process reviews, to employee and agent training on security, ethics and the appropriate use of customer information, all with the objective of reasonably controlling the collection, storage, access, use and disclosure of customer (as well as other) Qwest confidential information. The record indicates that other carriers have similar well-established programs in place.

Within the context of wide-ranging and multiple carrier controls of CPNI, the Commission should recalibrate the balance between regulatory prescription and management prerogative. The Commission should refrain from further CPNI regulation at this time. Rather, it should defer to carriers' professional judgment regarding what, if any, additional safeguards are necessary to reasonably protect CPNI. Such judgments will be informed by a carrier's own resource and risk assessments, as well as by their appreciation of any specific threats or hazards.

This is the sagest policy approach, particularly in a regulatory landscape in flux. Carriers increasingly operate in a competitive world of multiple suppliers, with waning common carrier regulation. Yet CPNI regulation is common carrier regulation. It is a Congressional and administrative intervention into the collection and use of information by but a handful of American businesses. To the extent possible, then, CPNI regulation should be moderate, in line with regulations of other industries, and highly correlated to predictable and material risks.

Such a regime would allow carriers to remain relatively free to operate unburdened by information-management costs not shared by other commercial enterprises and with some semblance of the flexibility enjoyed by them. And still there would be a place for enforcement. The Commission would remain poised to act swiftly to enforce Section 222 and the

Commission's corresponding rules in the event a carrier is found to have acted unreasonably with respect to its customer information.

II. NO ADDITIONAL CPNI RULES ARE NECESSARY

It bears remembering that this current aspect of the Commission's CPNI rulemaking was driven by regulatory concerns regarding "pretexting" and its attendant publicity. Pretexting involves a good guy, *i.e.*, a carrier employee trained to help and assist calling parties or a carrier-established online portal established to meet a customer need, and a bad guy, *i.e.*, a person whose purpose is to gain unauthorized access to information about another person, usually with an intent to use the information in a way that will cause harm to both an individual and the carrier. This fact pattern represents a fairly specific "evil" with regard to the unauthorized disclosure of customer information. Government-imposed "remedies" should be equally limited.

Qwest's[4] comments from 2006 bear repeating here to inform the discussion of additional CPNI safeguards, as suggested by the *2007 CPNI Further Notice*.

> Qwest, like all businesses accumulating customer account information and having routine customer contacts, strives to provide responsive, quality service in an "easy-to-do business with" environment. And Qwest, like all other businesses that manage account information, strives to balance customer convenience with necessary customer authentication and other security protections. Achieving the right balance is as much art as science. To determine the right balance, carriers like Qwest must consider a multitude of factors, including: (1) the volume of customer transactions they experience per week or per month or per year; (2) customer partiality for ease and convenience; (3) the nature of the risks involved, *e.g.*, "Are the risks occurring now or anticipated?"; "If now, what is the likelihood, frequency or the regularity of the risks?"; "What is the ability to manage the risks after they occur rather than in anticipation of them?"; and (4) the overall costs to the business and its customers of acting now, acting later or not acting at all. There is no perfect balance, no "one-size-fits-all" model. Rather, there are judgments and exercises of discretion that carriers should be accorded the right to make.

---

[4] This filing is made on behalf of Qwest Communications International Inc.'s common carrier companies, specifically Qwest Corporation (local exchange), Qwest Communications Corporation (long distance) and Qwest Wireless, Inc., collectively referred to as Qwest. In the event a point is being made with respect to a single company, that company will be identified by name.

> In the absence of a proven pattern of carrier conduct evidencing inadequate business practices or security protections, or facts evidencing carrier complicity with fraudulent conduct, carriers -- like other commercial businesses -- should be free to balance the costs and benefits of particular security measures when designing and implementing their information security architectures and protecting their informational assets, including customer information. Barring proof of significant carrier negligence or carelessness, the federal government should not impose business rules on the carrier-customer relationship that are not driven by product and service considerations and are not borne by other service providers or industries.[5]

Qwest continues to believe in the soundness of its earlier-stated position. Accordingly, we ask that the Commission refrain from promulgating any further CPNI rules.

A. No Additional CPNI Rules Should be Promulgated

1. Password Protection

Customers have choices about passwords. Qwest allows its customers to establish passwords with regard to their accounts. "In pursuit of its customer service goal, Qwest . . . accommodates a customer's choice to use a password with respect to access and release of customer information about them. The choice is the customer's; and those who do not want a password or consider them a burden do not have to have or manage one."[6]

In addition to the ability to choose a password, the Commission has now compelled customers to have and use a password in certain circumstances, regardless of a customer's preference. Passwords are now required with respect to the access and disclosure of call detail records ("CDRs") and online account access.

Qwest urges the Commission not to mandate any more extensive password-account requirement. The primary reason to act with restraint is because customers do not like passwords

---

[5] Qwest 2006 Comments at 3-4 (footnotes omitted).

[6] *Id.* at 21.

-- something the Commission acknowledges in its *April 2007 CPNI Order*.[7] Many individuals consider passwords an annoying hindrance rather than a necessary protection. This is even more true to the extent a person only occasionally or rarely interacts personally with a business, something that is typical in the world of telecommunications service providers.[8] Forcing customers to have or remember a password for infrequent encounters is highly likely to generate customer dissatisfaction, creating an overall negative carrier-customer experience rather than a positive one.

Similarly, passwords are not needed for "select" customer-carrier communications such as mentioned in the *2007 CPNI Further Notice* -- situations such as a change of address, a modification to a billing method or a change in service plan.[9] These are routine types of discussions between carrier service representatives and customers. Burdening these discussions with inquiries about "what is your password" and explaining the consequence of not having or remembering one weighs down easy communication and adds enormous transactional costs to the contact. These conversational barriers and economic burdens are unwarranted, especially since the Commission has already amended the CPNI rules to require after-the-fact notifications, *e.g.*, account activity such as change of address, change of password or back-up means of authentication, and changes to an online account.[10]

---

[7] *See April 2007 CPNI Order* at n.47, citing positively AT&T's Comments at 8-11 (AT&T referenced a Ponemon Institute study showing that the vast majority of respondents opposed the use of passwords; *see* Larry Ponemon, PhD, Data Security, Study on Passwords Reveals Most Forget, Must Reset Passwords Multiple Times, Privacy & Security Law, Vol. 5, No. 10 (March 6, 2006) at 8-9 and Centennial's Comments at 3-4.

[8] *See* Comments of Verizon, RM-11277, filed Oct. 31, 2005 at 3 ("a customer may not need to contact his carrier for many months, and when he does have a need to talk to the carrier, may have forgotten the password he selected.").

[9] *2007 CPNI Further Notice* ¶ 68.

[10] *April 2007 CPNI Order* ¶ 24.

And then there is the persistent "problem" of forgotten or misplaced passwords. Conversations between carriers and their customers that should be service oriented and comfortable can convert quickly into contentious interactions suggestive of interrogations. And to what end, particularly when a considerable body of CPNI lacks the kind of sensitivity associated with a CDR (*e.g.*, does a fraudster care if a customer has a "do not solicit" service, or used call waiting 3 times in the past month for a total charge of $2.25?).

Even if password-controlled communications were warranted in the case of CDRs (or other highly-sensitive information exchanges), burdening -- or evening eliminating -- routine carrier-customer exchanges about less sensitive information because of a predicate password barrier would enjoy little legal or policy support. And there certainly is no sound public policy reason to impose access controls on customers that they dislike and, accordingly, will not use efficiently or happily.

Imposition of a "totally-password-controlled environment" for access and disclosure of CPNI would target carriers for regulatory prescriptions unknown in American business. Such radical action would fail to provide consumer "protection" in any satisfactory sense because the need for the protection (as to less-sensitive CPNI) would remain oblique; and the target of the protection (the consumer) would not welcome it. Rather, it would catapult consumers of carrier services into the most unwelcoming commercial relationship they encounter among their world of service providers, including providers of health and financial services. Such action would be unfair to such consumers and their serving carriers alike, and the Commission should not resolve the balance in that manner.

2. Audit Trails

Qwest supports the incorporation of audit functionalities into an overall information security program; and it has said so previously.[11] But the creation of audit trails is a single aspect of a carrier's more comprehensive security program designed to protect its confidential information.[12] For example, Qwest's information security program incorporates a variety of preventive features (*e.g.*, training, network-intrusion monitors; firewalls to avoid penetrations; employee password protections[13] to avoid unauthorized access).[14]

Audit functionalities are built into information security programs to collect information today that might be of use to a carrier tomorrow, particularly in investigating compromised controls or failed safeguards.[15] How much information should be collected and stored[16] and what

---

[11] Qwest 2006 Comments at 29.

[12] Qwest provided a general description of its information security program and elements in its previously-filed comments. *See id.* at 25-29. Qwest "also employs anti-virus and anti-spam technologies at multiple computing levels including e-mail, desktop and server levels, in efforts to minimize the risk of malicious code introduction and hacking events. Qwest's multi-layered defense also includes web-content filtering and blocking, instant messaging controls and desktop firewalls to minimize opportunities for infection by spyware, other malicious software ("malware") and individual hacker attacks." *Id.* at 28-29.

[13] The BOCs, and later GTE, were required by the Commission's *Computer II* and ONA rules, to incorporate password-identification protection in to their "primary" customer information databases. *See, e.g., In the Matter of Filing and Review of Open Network Architecture Plans*, Memorandum Opinion and Order, 8 FCC Rcd 2606, 2610 ¶ 18 (1993); *In the Matter of Filing and Review of Open Network Architecture Plans*, Memorandum Opinion and Order, 5 FCC Rcd 3103, 3118-19 ¶¶ 129-37 (1990).

[14] Qwest "also uses audit trails (sometimes called "logs") at both the application and computer operating system levels to collect information about access to data by both application users and system administrators (the latter sometimes called "privileged users")." *See* Qwest 2006 Comments at 30.

[15] Widely-published information and warnings about the existence of auditing and monitoring capabilities act as a deterrent to inappropriate information access and disclosure. Still, audit trails primarily serve an investigative function -- to provide evidence to address system breaches or failures, evidence that is helpful in root-cause analyses, for example.

kinds of future incidents and investigations might make use of that information are highly correlated to a business' overall governance,[17] risk tolerance and resources. Managers make decisions about the relative benefits of instituting up-front access controls versus implementing use controls, where the use controls will be buttressed by available audit tools that can be utilized later to determine if the use controls lack reliability.

Once the matter of scope is resolved, there is the art of designing an optimum audit architecture. Among the factors to be considered are: (a) the transactions to be identified and tracked; (b) the identification of the specific data associated with each transactional event to be recorded, stored and retained; (c) the number of times stale information is sought to be retrieved over periods of time; (d) the override process (*e.g.*, writing over stale data with new data so as to not lose memory function); and (e) the dynamism of the forensic investigation process (*e.g.*, some processes are more suited to "proof" through transactional data than are others).

Given the complex factors that inform any decision about the role of audit capabilities in a larger information security program, it is patent that utility regulators lack the professional subject matter expertise to make these decisions for a single carrier, let alone an entire telecommunications industry. Moreover, changes to the mix of preventative *versus* audit functions can be very expensive even for one carrier; the costs would be enormous for an entire

---

[16] For every bit of information collected by an audit trail/log, there is a correlative decision about where and how long to keep such information and with what controls. Information in audit trails, to the extent the trail itself includes customer information, becomes a "database" of warehoused information that might be subject to invasion or breaches.

[17] For example, as Qwest advised previously, it has a strong training program, as well as a governance structure infused with "(3) controls in the nature of directives admonishing its employees to act lawfully and ethically and to report unlawful or unethical behavior, supplemented by investigations in the event of alleged wrongdoing." Qwest 2006 Comments at 30.

communications industry. Such changes can also create unforeseen, cascading consequences for both the design and the cost of the larger information security program.

Clearly, prescriptions of specific audit trail designs or functionalities for carriers would impose tremendous burdens with no discernible commensurate benefit to the public or law enforcement community.[18] In the absence of compelling evidence of serious public harm, no such prescriptions should occur. Not only is there no such evidence. The record evidence is to the contrary.

The current record shows that carriers have implemented and use audit capabilities, although specific audit types and deployment regimes undoubtedly differ as among carriers of different sizes and business models. As Qwest previously stated,

> Larger carriers' audit functionalities, functionalities shared by Qwest, can generally track when an employee accesses a system or database and when he/she leaves. This information can later be used to discern whether a particular employee accessed a particular system with -- or without -- authorization. Such information can be used, in turn, to ensure that employees who are *not* authorized to access systems that contain customer information do not do so. And if some employees do act contrary to established carrier practices, they will be subject to the carrier's express disciplinary plan,[19] which likely would include dismissal where warranted.
>
> Beyond audit functionalities that record basic employee entry into and exit from a system, many carriers likely have more sophisticated audit controls. Larger carriers, like Qwest, might have audit tools that "mark" a specific record with a unique employee identifier when an employee accesses a customer account. And like Qwest they might have audit technology that tracks not only the fact that a service representative accessed

---

[18] The Commission asks whether a particular type of audit trail would assist law enforcement with criminal investigations. *2007 CPNI Further Notice* ¶ 69. In Qwest's opinion, law enforcement's needs are most likely met by those audit functionalities a carrier determines to deploy, based on its particular business model and commercial considerations. Qwest routinely cooperates with law enforcement in the prosecution of illegal conduct as required or permitted by law. We are unaware of any dissatisfaction by law enforcement of Qwest's audit capabilities.

[19] 47 C.F.R. § 64.2009(b); *1998 CPNI Order*, 13 FCC Rcd at 8198 ¶ 198; and *Notice of Proposed Rulemaking*, CC Docket No. 96-115 and RM-11277, 21 FCC Rcd 1782, 1785 ¶ 7 and n.18 (2006).

an account (*e.g.*, a log of entry/exit) but also requires notes explaining the reason for access to the customer record, as well as any action taken.[20]

The matter of design and implementation of audit functionalities is clearly complex. Unless the Commission has evidence before it that a carrier is *failing to protect* the proprietary information of its customers (*see* Section 222(a)), *and* that such failure is associated with a lack of basic audit trails that a reasonable person/carrier would be expected to have, the Commission should not act in this area. As Qwest previously stated, it would likely be a rare and isolated instance such a demonstration could be made about a carrier.[21]

3. Physical Safeguards

The *2007 CPNI Further Notice* inquires about physical safeguards associated with customer information. Those safeguards seem to include both tangible protections (like gates and locks, and encrypted laptops) as well as more intangible "physical" safeguards, such as the encryption of information in transit. Qwest addresses both concepts and associated controls below. Qwest's Code of Conduct stresses the seriousness of protecting Qwest's assets, including its confidential information.

Physical Locations. As previously noted, Qwest retail sales locations and data centers are protected by physical security controls that act to safeguard access to and improper disclosure of Qwest confidential information, including CPNI.[22] Qwest-owned computers that are used in

---

[20] Qwest 2006 Comments at 13-14.

[21] "After the passage of the Sarbanes-Oxley Act of 2002 ("SOX") those claiming that a publicly-held company's security controls pertaining to financial systems and data (which included significant amounts of customer information) are inadequate would have an exceedingly difficult time proving it. Such companies are required to have adequate controls in place to ensure the confidentiality and integrity of financial information, supported by an annual certification from an internal controller and an attestation from an independent body. In a very material way, SOX buttresses those CPNI safeguards that the Commission itself established." Qwest 2006 Comments at 8 (footnotes omitted).

[22] *Id.* at 30.

its on-site locations have been updated to reduce the amount of CPNI stored on them. Qwest also inventories backup tapes from applications that may contain CPNI and stores the tapes in physically-secured locations.

Information Transfers. Qwest has relationships with third parties where customer information is exchanged. Besides the predicate safeguard, *i.e.*, knowing whom you are doing business with, Qwest's third-party relationships include information security controls such as contract provisions: (1) requiring that information be treated confidentially and be safeguarded to the same extent the third party would protect its own information; (2) requiring that the vendor abide by its own corporate Code of Conduct; (3) requiring that confidential information be destroyed or returned upon Qwest's request; (4) specifying the manner and means of the information exchange, taking into consideration whether the information is expected to be in transit through a public-media (such as the Internet) or a private one (such as private line, encrypted disc); and, if appropriate, (5) granting audit rights. Qwest also provides its vendors with a link to its Supplier Code, which is currently being revised (*see* www.qwest.com/about/company/ethics/files/SuppliersBrochure.pdf.

Qwest's safeguards are appropriate ones and are likely similar to safeguards implemented by carriers around the country. Of course, each carrier will have slightly different provisions, depending on its history and the philosophy of its organization.

Qwest reiterates the argument here, in the context of physical safeguards of customer information that it made above in the context of mandated audit trails. Unless the Commission has evidence before it that a carrier is *failing to protect* the proprietary information of its customers (*see* Section 222(a)), *and* that such failure is caused by the lack of basic physical

controls that a reasonable person/carrier would be expected to have, the Commission should not act in this area.

4. Limiting Data Retention

The *2007 CPNI Further Notice* seeks comment on the need for rules requiring carriers to limit data retention. Qwest has addressed this matter before (with respect to the Electronic Privacy Information Center ("EPIC" Petition).[23] The answer is "no." Customer information does not merely reflect transactions to which the customer is a party; it is a carrier asset and information that is incorporated in a wide variety of carrier business records. This information is used for many purposes, not the least of which is to provision service, bill accurately (thus generating revenue), provide customer service, address litigation claims and other disputes, and prove the legitimacy of its claims for tax and other income purposes.

As stated previously, the data retention requirements of most companies already are crafted to maintain the information for no longer than the business deems reasonably necessary.

> Qwest, like other carriers, has implemented a formal records management policy, document retention schedule, and associated procedures that apply to all of Qwest's business operations, as required by 47 C.F.R. § 42. Customer information, such as call detail records, is considered sales and services records that Qwest keeps for a minimum of two years.
>
> Qwest often extends its default retention period as a result of legal or tax holds that override its general retention schedule. Because customer-usage detail information is of substantial significance to billed revenues, Qwest retains these usage detail/billing records for the amount of time associated with Internal Revenue Service or applicable state tax holds **plus** an additional year. This often leads to retention periods that can range from seven to fifteen years.[24]

A rule that tried to accommodate all different types of carriers (and non-carriers such as VoIP providers), as well as all state and federal rules and regulations pertaining to the ability to

---

[23] *Id.* at 36-37.

[24] *Id.* at 17 (footnote omitted, referred to 47 C.F.R. § 42.6 (carriers must maintain billing records for 18 months)).

prove representations (often what retained data is used for), would have as its content a broadly-worded prescription, *e.g.*, "Carriers shall not keep data beyond the point where it is useful to the carrier for some legal, policy or legitimate business purpose." Such a rule lacks, obviously, a specified "maximum amount of time that a carrier should be able to retain customer records," a question raised by the *2007 CPNI Further Notice*.[25] On the other hand, such a rule does not change or modify the business practices of most carriers (Qwest believes) and, therefore, is totally unneeded.[26]

As an "alternative" to limiting data retention, the *2007 CPNI Further Notice* inquires about possible "de-identify[ing] customer records after a certain period."[27] The costs of such an initiative would be huge -- and, as a matter of legal compulsion, would be suffered only by common carriers.[28] Moreover, de-identifying information could create an unresolvable tension for carriers attempting to meet multiple legal obligations. For example, in litigation contexts, parties are routinely required to preserve and produce electronically-stored information in its original state. De-identifying information could be considered an "alteration" of that state.

It is not, of course, that separating information from a customer's identity cannot be done technically. Surely, it can. But for carriers that use multiple systems (indeed are the product of multiple, merged companies) it certainly cannot be done cheaply. While it may be that carriers

---

[25] *2007 CPNI Further Notice* ¶ 71.

[26] As is noted in the *2007 CPNI Further Notice* and its reference to Cingular's Comments, pretexters generally are interested in newer records and information -- not older ones, to which a data retention obligation would be directed. Thus, mandating the destruction of older records does not materially advance CPNI protection in such a context.

[27] *2007 CPNI Further Notice* ¶ 71. How this inquiry is different from the EPIC proposal regarding the de-identification of records, and the Commission's earlier request for comment, is not clear to Qwest. Qwest opposed the concept earlier. Qwest 2006 Comments at 16-18.

[28] In addition to creating the de-identification functionality, carriers would simultaneously have to create and maintain some kind of "key" to re-identify the customer associated with the anonymized information should it become necessary.

with newer, more nimble technologies could separate the information with greater facility, there would be a cost even for them.

Nowhere has a proponent of this notion proven that the undeniable costs of pursuing it would be outweighed by an identifiable public benefit stemming from it. Until such demonstration is made, the Commission should not prescribe a system functionality of common carriers that is neither commonplace nor mature in its development.

B. Protection of Information Stored in Mobile Communications Devices

The *2007 CPNI Further Notice* asks what actions should be taken, if any, to secure the privacy of information stored on mobile devices.[29] These days that information can include not only the kind of commercially and financially-sensitive information referenced by the *2007 CPNI Further Notice*,[30] but more parochial information such as name and telephone contact information, text messages, visited internet sites, and music and video access information.

The Commission asks about both customer capabilities for removing or erasing information as well as carrier capabilities. Customers have considerable abilities to remove personal information from their wireless handsets. Using their Options Menu, they can easily erase the contacts, pictures, and other personal data. This will generally return the telephone to what is called an "out of the box configuration."

In addition, while Qwest cannot speak for every mobile service provider, the vast majority of the phones Qwest provides to customers today have a reverse logistics hidden

---

[29] *2007 CPNI Further Notice* ¶ 72.

[30] *Id.* at n.208 (referencing a newspaper article that discussed a discarded mobile device that included the specifics of a multi-million dollar federal transportation contract, bank account information, and passwords).

sequence in them that can be used to return the handset to an "out of the factory" configuration. Qwest uses this function on every handset it receives back at its fulfillment center.[31]

The *2007 CPNI Further Notice* might also be seeking information about the ability of carriers, such as Qwest, to remove personal information from a mobile handset remotely -- for example, if a phone is lost or stolen. Qwest knows of no current industry standards, or even widely-accepted technologies, regarding such capability. Indeed, Qwest is aware of only a single manufacturer with a single handset that currently has this capability, and even then it is a feature that must be activated by the customer. While such "remote zapping" functionality is currently being built into some small, hand-held computing devices, Qwest believes that the capability is not widespread and is not currently planned for most mobile handsets.

III. CONCLUSION

Qwest appreciates the Commission's continued dedication to the principles of consumer protection, including the protection of customer information. But further amendments to the CPNI rules are not necessary to accomplish that goal. Existing CPNI rules, coupled with carriers' statutory duty to protect customer proprietary information (47 U.S.C. § 222(a)), remain more than sufficient government articulation of carriers' obligations.

Rather, the Commission should acknowledge the laudatory efforts of carriers across the country to craft, maintain, and evolve robust, reasonable and most-often effective information security controls in light of a constantly and increasingly threatening landscape. Costly and operationally burdensome government regulations should not be inflicted on well-intentioned carriers in the absence of proven public interest benefits.

---

[31] The basic difference between what the customer can easily do and what a carrier might do in addition through the reverse logistics function is that a carrier will remove the assigned MDN MSID (Phone Number) from the device in addition to the personal information the customer could control removing.

Instead, regulatory action should be confined to those bad actors, *e.g.*, to carriers demonstrably lax about their information security, customer authentication or information-disclosure practices. Carriers that demonstrate a course of conduct reflecting non-compliance with their statutory and regulatory duties to protect customer information should be targets of Commission enforcement action.

Respectfully submitted,

QWEST COMMUNICATIONS
INTERNATIONAL INC.

By: Kathryn Marie Krause
Craig J. Brown
Kathryn Marie Krause
Suite 950
607 14th Street, N.W.
Washington, DC 20005
303-383-6651

July 9, 2007

CERTIFICATE OF SERVICE

I, Richard Grozier, do hereby certify that I have caused the foregoing **COMMENTS OF QWEST COMMUNICATIONS INTERNATIONAL INC. TO FURTHER NOTICE OF PROPOSED RULEMAKING** to be 1) filed with the FCC via its Electronic Comment Filing System in CC Docket No. 96-115 and WC Docket No. 04-36; 2) served via e-mail on Ms. Janice Myles, Competition Policy Division, Wireline Competition Bureau at janice.myles@fcc.gov; and 3) served via e-mail on the FCC's duplicating contractor Best Copy and Printing, Inc. at fcc@bcpiweb.com.

/s/Richard Grozier

July 9, 2007